DATE(S) ISSUED:
02/14/2012

SUBJECT:
Vulnerabilities in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (MS12-015)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Visio Viewer 2010, a program used for creating flowcharts and diagrams. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
Microsoft Visio Viewer 2010

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: Medium

DESCRIPTION:
Five vulnerabilities have been identified in Microsoft Visio that could allow remote code execution. These vulnerabilities are caused due to the way Microsoft Visio validates attributes when handling a specially crafted Visio file (.VSD). They can also be exploited via an email attachment or through the Web. In the email based scenario, the user would have to open the specially crafted Visio file as an email attachment. In the Web based scenario, a user would visit a website and then open the specially crafted Visio file that is hosted on the page.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Microsoft:
http://technet.microsoft.com/en-us/security/bulletin/ms12-015

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0019
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0020
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0136
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0137
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0138

Security Focus:
http://www.securityfocus.com/bid/